A Unified Deep Learning Anomaly Detection and Classification Approach for Smart Grid Environments

Year: 2021 | Citations: 186 | Authors: Ilias Siniosoglou, Panagiotis I. Radoglou-Grammatikis, G. Efstathopoulos, Panagiotis E. F

Abstract

The interconnected and heterogeneous nature of the next-generation Electrical Grid (EG), widely known as Smart Grid (SG), bring severe cybersecurity and privacy risks that can also raise domino effects against other Critical Infrastructures (CIs). In this paper, we present an Intrusion Detection System (IDS) specially designed for the SG environments that use Modbus/Transmission Control Protocol (TCP) and Distributed Network Protocol 3 (DNP3) protocols. The proposed IDS called MENSA (anoMaly dEtection aNd claSsificAtion) adopts a novel Autoencoder-Generative Adversarial Network (GAN) architecture for (a) detecting operational anomalies and (b) classifying Modbus/TCP and DNP3 cyberattacks. In particular, MENSA combines the aforementioned Deep Neural Networks (DNNs) in a common architecture, taking into account the adversarial loss and the reconstruction difference. The proposed IDS is validated in four real SG evaluation environments, namely (a) SG lab, (b) substation, (c) hydropower plant and (d) power plant, solving successfully an outlier detection (i.e., anomaly detection) problem as well as a challenging multiclass classification problem consisting of 14 classes (13 Modbus/TCP cyberattacks and normal instances). Furthermore, MENSA can discriminate five cyberattacks against DNP3. The evaluation results demonstrate the efficiency of MENSA compared to other Machine Learning (ML) and Deep Learning (DL) methods in terms of Accuracy, False Positive Rate (FPR), True Positive Rate (TPR) and the F1 score.